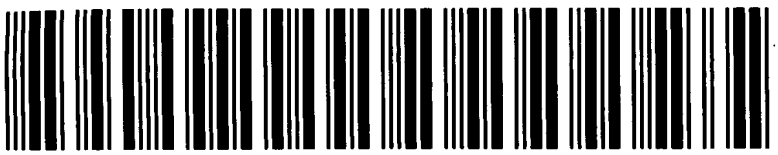
IDS REFERENCES



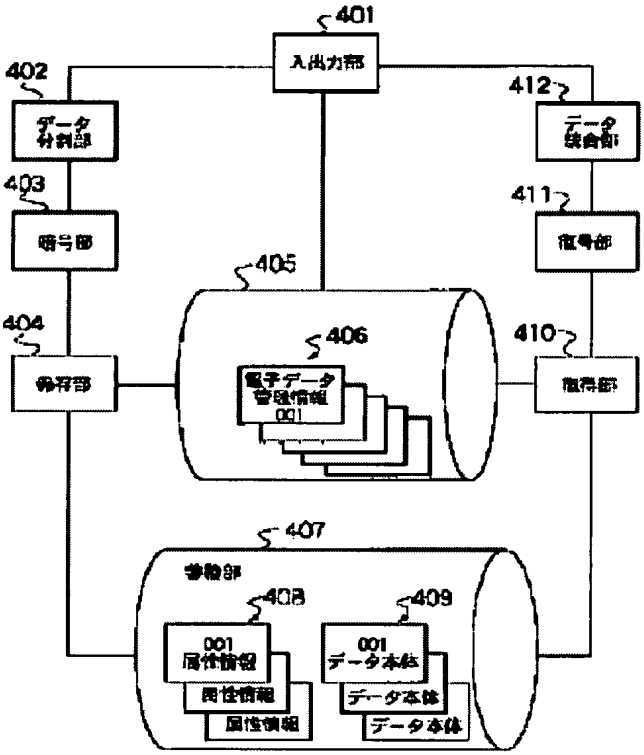
☒ FOR

ELECTRONIC DATA MANAGEMENT DEVICE AND METHOD AND RECORDING MEDIUM RECORDING ELECTRONIC DATA MANAGEMENT PROGRAM

Publication number: JP2000172566
Publication date: 2000-06-23
Inventor: NAGATA TAKAOKI; HORIOKA TSUTOMU; WATABE YASUHIKO; SONEHARA NOBORU
Applicant: NIPPON TELEGRAPH & TELEPHONE
Classification:
- international: ***G06F12/14; G06F21/24; G09C1/00;*** **G06F12/14; G06F21/00; G09C1/00;** (IPC1-7): G06F12/14; G09C1/00
- European:
Application number: JP19980347370 19981207
Priority number(s): JP19980347370 19981207

Abstract of **JP2000172566**

PROBLEM TO BE SOLVED: To provide an electronic data management device and a method which can surely prevent the third parties from reading and using by stealth of the electronic data and also to provide a recording medium which records an electronic data management program. SOLUTION: A file which is inputted via an input/output part 401 is separated into the attribute information and a data main body at a data dividing part 402 and then enciphered at an enciphering part 403 by means of respectively different cipher keys. The enciphered attribute information and data main body are stored in different storing parts of a storing part 407 via a preserving part 404 and then an electronic data management information which shows the storing parts of those attribute information and main body is registered in a managing part 405. In regard to acquisition of the electronic data, the enciphered attribute information and data main body are acquired from the part 407 via an acquiring part 410 based on the management information registered at the part 405. Then the ciphered attribute information and data main body are decoded at a decoding part 411, integrated together at a data integrating part 412 and outputted via the part 401.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－172566
（P2000－172566A）
(43)公開日　平成12年６月23日(2000.6.23)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｇ０６Ｆ　12/14	３２０	Ｃ０６Ｆ　12/14	３２０Ｂ	５Ｂ０１７
Ｇ０９Ｃ　1/00	６６０	Ｃ０９Ｃ　1/00	６６０Ｄ	５Ｊ１０４
				９Ａ００１

審査請求　未請求　請求項の数18　ＯＬ　（全９頁）

(21)出願番号　特願平10－347370

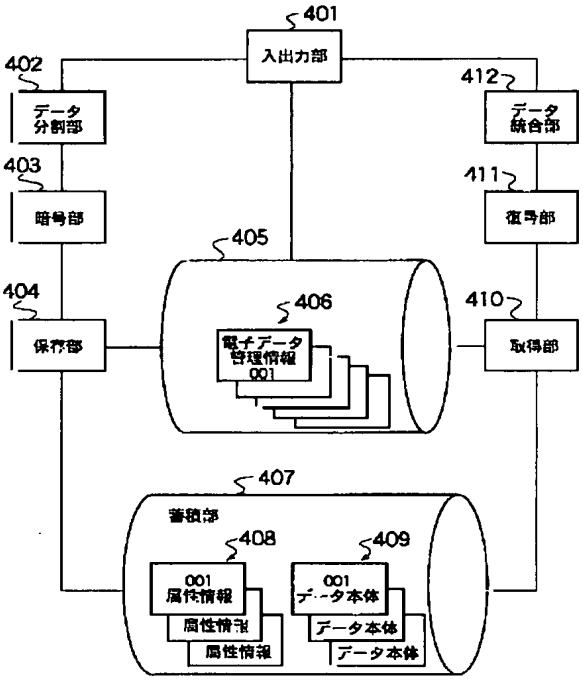
(22)出願日　平成10年12月７日(1998.12.7)

(71)出願人　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目３番１号
(72)発明者　永田　誉興
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内
(72)発明者　堀岡　力
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内
(74)代理人　100083806
弁理士　三好　秀和　（外１名）

最終頁に続く

(54)【発明の名称】　電子データ管理装置および方法と電子データ管理プログラムを記録した記録媒体

(57)【要約】
【課題】　第三者による電子データの閲覧、盗用等を適確に防止し得る電子データ管理装置および方法と電子データ管理プログラムを記録した記録媒体を提供する。
【解決手段】　入出力部４０１から入力されたファイルはデータ分割部４０２で属性情報とデータ本体に分離され、暗号部４０３でそれぞれ異なる暗号鍵を用いて暗号化される。この暗号化された属性情報とデータ本体は保存部４０４により蓄積部４０７のそれぞれ別々の格納場所に保存され、その格納場所を示す電子データ管理情報は管理部４０５に登録される。電子データの取得では、管理部４０５に登録されている管理情報に基づいて蓄積部４０７から暗号化された属性情報とデータ本体を取得部４１０により取得する。この暗号化された属性情報とデータ本体を復号部４１１でそれぞれ復号する。この復号された属性情報とデータ本体をデータ統合部４１２で統合し、入出力部４０１から出力する。



【特許請求の範囲】

【請求項１】　属性情報と本体情報からなる電子データを管理する電子データ管理装置であって、
電子データを保存する際に該電子データの利用者を特定するための利用者特定情報と前記電子データを同定するためのデータ同定情報の入力を要求する保存時入力要求手段と、
前記電子データを属性情報と本体情報に分割するデータ分割手段と、
この分割された属性情報と本体情報を各々異なる記憶領域に格納する格納手段と、
前記利用者特定情報、前記電子データに属する前記属性情報および本体情報の前記格納手段におけるそれぞれの格納位置を統合して管理情報として記録管理する記録管理手段と、
前記電子データを利用する際に該電子データの利用を要求する利用者を特定するための利用者要求情報と前記電子データを同定するためのデータ同定情報の入力を要求する利用時入力要求手段と、
前記利用者要求情報と前記利用者特定情報が一致する場合、前記管理情報を参照して前記格納手段から属性情報と本体情報を読み出し、この読み出した属性情報と本体情報を統合する統合手段とを有し、
前記電子データが格納されているときに前記本体情報の所在のみを利用者に開示することを特徴とする電子データ管理装置。

【請求項２】　前記格納手段は、前記属性情報と本体情報を各々異なる記憶領域に格納するに当り、前記利用者特定情報に基づいた暗号化情報を用いて、前記属性情報と本体情報のいずれか一方または両方を暗号化する暗号化手段を有し、
前記統合手段は、前記属性情報と本体情報を統合するに当り、前記利用者要求情報に基づいた復号化情報を用いて、前記暗号化されているいずれか一方または両方の属性情報と本体情報を復号化する復号化手段を有することを特徴とする請求項１記載の電子データ管理装置。

【請求項３】　前記暗号化情報および復号化情報は、前記属性情報および本体情報に対して異なる情報であることを特徴とする請求項２記載の電子データ管理装置。

【請求項４】　属性情報と本体情報からなる電子データを管理する電子データ管理装置であって、電子データを属性情報と本体情報に分割し、この分割された属性情報と本体情報をそれぞれ異なる記憶領域に格納する格納手段を有することを特徴とする電子データ管理装置。

【請求項５】　前記格納手段は、前記属性情報と本体情報をそれぞれ異なる記憶領域に格納するに当り、前記属性情報と本体情報のいずれか一方または両方を暗号化する暗号化手段を有することを特徴とする請求項４記載の電子データ管理装置。

【請求項６】　前記暗号化手段は、前記電子データの利用者毎に生成された暗号鍵を用いて暗号化を行うことを特徴とする請求項５記載の電子データ管理装置。

【請求項７】　属性情報と本体情報からなる電子データを管理する電子データ管理方法であって、
電子データを保存する際に該電子データの利用者を特定するための利用者特定情報と前記電子データを同定するためのデータ同定情報の入力を要求する保存時入力要求過程と、
前記電子データを属性情報と本体情報に分割するデータ分割過程と、
この分割された属性情報と本体情報を各々異なる記憶領域に格納する格納過程と、
前記利用者特定情報、前記電子データに属する前記属性情報および本体情報の前記格納手段におけるそれぞれの格納位置を統合して管理情報として記録管理する記録管理過程と、
前記電子データを利用する際に該電子データの利用を要求する利用者を特定するための利用者要求情報と前記電子データを同定するためのデータ同定情報の入力を要求する利用時入力要求過程と、
前記利用者要求情報と前記利用者特定情報が一致する場合、前記管理情報を参照して前記格納手段から属性情報と本体情報を読み出し、この読み出した属性情報と本体情報を統合する統合過程とを有し、
前記電子データが格納されているときに前記本体情報の所在のみを利用者に開示することを特徴とする電子データ管理方法。

【請求項８】　前記格納過程は、前記属性情報と本体情報を各々異なる記憶領域に格納するに当り、前記利用者特定情報に基づいた暗号化情報を用いて、前記属性情報と本体情報のいずれか一方または両方を暗号化する暗号化過程を有し、
前記統合過程は、前記属性情報と本体情報を統合するに当り、前記利用者要求情報に基づいた復号化情報を用いて、前記暗号化されているいずれか一方または両方の属性情報と本体情報を復号化する復号化過程を有することを特徴とする請求項７記載の電子データ管理方法。

【請求項９】　前記暗号化情報および復号化情報は、前記属性情報および本体情報に対して異なる情報であることを特徴とする請求項８記載の電子データ管理方法。

【請求項１０】　属性情報と本体情報からなる電子データを管理する電子データ管理方法であって、電子データを属性情報と本体情報に分割し、この分割された属性情報と本体情報をそれぞれ異なる記憶領域に格納する格納過程を有することを特徴とする電子データ管理方法。

【請求項１１】　前記格納過程は、前記属性情報と本体情報をそれぞれ異なる記憶領域に格納するに当り、前記属性情報と本体情報のいずれか一方または両方を暗号化する暗号化過程を有することを特徴とする請求項１０記載の電子データ管理方法。

【請求項１２】　前記暗号化過程は、前記電子データの利用者毎に生成された暗号鍵を用いて暗号化を行うことを特徴とする請求項１１記載の電子データ管理方法。
【請求項１３】　属性情報と本体情報からなる電子データを管理する電子データ管理プログラムを記録した記録媒体であって、
電子データを保存する際に該電子データの利用者を特定するための利用者特定情報と前記電子データを同定するためのデータ同定情報の入力を要求する保存時入力要求過程と、
前記電子データを属性情報と本体情報に分割するデータ分割過程と、
この分割された属性情報と本体情報を各々異なる記憶領域に格納する格納過程と、
前記利用者特定情報、前記電子データに属する前記属性情報および本体情報の前記格納手段におけるそれぞれの格納位置を統合して管理情報として記録管理する記録管理過程と、
前記電子データを利用する際に該電子データの利用を要求する利用者を特定するための利用者要求情報と前記電子データを同定するためのデータ同定情報の入力を要求する利用時入力要求過程と、
前記利用者要求情報と前記利用者特定情報が一致する場合、前記管理情報を参照して前記格納手段から属性情報と本体情報を読み出し、この読み出した属性情報と本体情報を統合する統合過程とを有し、
前記電子データが格納されているときに前記本体情報の所在のみを利用者に開示することを特徴とする電子データ管理プログラムを記録した記録媒体。
【請求項１４】　前記格納過程は、前記属性情報と本体情報を各々異なる記憶領域に格納するに当り、前記利用者特定情報に基づいた暗号化情報を用いて、前記属性情報と本体情報のいずれか一方または両方を暗号化する暗号化過程を有し、
前記統合過程は、前記属性情報と本体情報を統合するに当り、前記利用者要求情報に基づいた復号化情報を用いて、前記暗号化されているいずれか一方または両方の属性情報と本体情報を復号化する復号化過程を有することを特徴とする請求項１３記載の電子データ管理プログラムを記録した記録媒体。
【請求項１５】　前記暗号化情報および復号化情報は、前記属性情報および本体情報に対して異なる情報であることを特徴とする請求項１４記載の電子データ管理プログラムを記録した記録媒体。
【請求項１６】　属性情報と本体情報からなる電子データを管理する電子データ管理方法であって、電子データを属性情報と本体情報に分割し、この分割された属性情報と本体情報をそれぞれ異なる記憶領域に格納する格納過程を有することを特徴とする電子データ管理プログラムを記録した記録媒体。
【請求項１７】　前記格納過程は、前記属性情報と本体情報をそれぞれ異なる記憶領域に格納するに当り、前記属性情報と本体情報のいずれか一方または両方を暗号化する暗号化過程を有することを特徴とする請求項１６記載の電子データ管理プログラムを記録した記録媒体。
【請求項１８】　前記暗号化過程は、前記電子データの利用者毎に生成された暗号鍵を用いて暗号化を行うことを特徴とする請求項１７記載の電子データ管理プログラムを記録した記録媒体。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、電子データを安全に管理する電子データ管理装置および方法と電子データ管理プログラムを記録した記録媒体に関する。
【０００２】
【従来の技術】パソコン等に代表される電子計算機は個人的に利用するという性質上、個人ユーザ毎に電子データを管理する機能を備えていない。そのため、悪意のある第三者は容易に電子計算機を起動し、隠蔽しておきたい電子データを勝手に閲覧取得することが可能である。更に従来の個人利用を目的とした電子計算機であっても、ネットワークを利用した情報共有が進み、ネットワーク端末としても複数ユーザが共同利用する環境になってきている。それにもかかわらず、電子データの管理が十分に行われていない。
【０００３】
【発明が解決しようとする課題】パソコン等の個人ユーザ向け電子計算機においては、ユーザ自身によって電子データの安全性を確保する必要がある。しかしながら、ユーザは煩わしさ等のため何の対処もしないことが多く、悪意のある第三者により電子データの盗用、閲覧等が行われ易いという問題がある。この原因としては、電子データ自体が手を加えられずに保存されていることが挙げられる。
【０００４】本発明は、上記に鑑みてなされたもので、その目的とするところは、第三者による電子データの閲覧、盗用等を適確に防止し得る電子データ管理装置および方法と電子データ管理プログラムを記録した記録媒体を提供することにある。
【０００５】
【課題を解決するための手段】上記目的を達成するため、請求項１記載の本発明は、属性情報と本体情報からなる電子データを管理する電子データ管理装置であって、電子データを保存する際に該電子データの利用者を特定するための利用者特定情報と前記電子データを同定するためのデータ同定情報の入力を要求する保存時入力要求手段と、前記電子データを属性情報と本体情報に分割するデータ分割手段と、この分割された属性情報と本体情報を各々異なる記憶領域に格納する格納手段と、前記利用者特定情報、前記電子データに属する前記属性情

報および本体情報の前記格納手段におけるそれぞれの格納位置を統合して管理情報として記録管理する記録管理手段と、前記電子データを利用する際に該電子データの利用を要求する利用者を特定するための利用者要求情報と前記電子データを同定するためのデータ同定情報の入力を要求する利用時入力要求手段と、前記利用者要求情報と前記利用者特定情報が一致する場合、前記管理情報を参照して前記格納手段から属性情報と本体情報を読み出し、この読み出した属性情報と本体情報を統合する統合手段とを有し、前記電子データが格納されているときに前記本体情報の所在のみを利用者に開示することを要旨とする。

【0006】請求項1記載の本発明にあっては、電子データを保存する際にパスワード等の利用者特定情報とファイル名等のデータ同定情報の入力を要求し、電子データを属性情報と本体情報に分割し、この属性情報と本体情報を各々異なる記憶領域に格納し、利用者特定情報、属性情報および本体情報のそれぞれの格納位置を統合して管理情報として記録管理し、また電子データを利用する際にデータ利用者を特定する利用者要求情報とデータ同定情報の入力を要求し、利用者要求情報と利用者特定情報が一致する場合、管理情報を参照して属性情報と本体情報を読み出し、この属性情報と本体情報を統合し、電子データが格納されているときに本体情報の所在のみを利用者に開示する。

【0007】また、請求項2記載の本発明は、請求項1記載の発明において、前記格納手段が、前記属性情報と本体情報を各々異なる記憶領域に格納するに当り、前記利用者特定情報に基づいた暗号化情報を用いて、前記属性情報と本体情報のいずれか一方または両方を暗号化する暗号化手段を有し、前記統合手段が、前記属性情報と本体情報を統合するに当り、前記利用者要求情報に基づいた復号化情報を用いて、前記暗号化されているいずれか一方または両方の属性情報と本体情報を復号化する復号化手段を有することを要旨とする。

【0008】請求項2記載の本発明にあっては、属性情報と本体情報を各々異なる記憶領域に格納するに当り、利用者特定情報に基づいた暗号化情報を用いて属性情報と本体情報のいずれか一方または両方を暗号化し、また属性情報と本体情報を統合するに当り、利用者要求情報に基づいた復号化情報を用いて、前記暗号化されているいずれか一方または両方の属性情報と本体情報を復号化する。

【0009】更に、請求項3記載の本発明は、請求項2記載の発明において、前記暗号化情報および復号化情報が、前記属性情報および本体情報に対して異なる情報であることを要旨とする。

【0010】請求項3記載の本発明にあっては、暗号化情報および復号化情報は属性情報および本体情報に対して異なる情報である。

【0011】請求項4記載の本発明は、属性情報と本体情報からなる電子データを管理する電子データ管理装置であって、電子データを属性情報と本体情報に分割し、この分割された属性情報と本体情報をそれぞれ異なる記憶領域に格納する格納手段を有することを要旨とする。

【0012】請求項4記載の本発明にあっては、電子データを属性情報と本体情報に分割し、この分割された属性情報と本体情報をそれぞれ異なる記憶領域に格納するため、電子データを安全に保存することができる。

【0013】また、請求項5記載の本発明は、請求項4記載の発明において、前記格納手段が、前記属性情報と本体情報をそれぞれ異なる記憶領域に格納するに当り、前記属性情報と本体情報のいずれか一方または両方を暗号化する暗号化手段を有することを要旨とする。

【0014】請求項5記載の本発明にあっては、属性情報と本体情報をそれぞれ異なる記憶領域に格納するに当り、属性情報と本体情報のいずれか一方または両方を暗号化する。

【0015】更に、請求項6記載の本発明は、請求項5記載の発明において、前記暗号化手段が、前記電子データの利用者毎に生成された暗号鍵を用いて暗号化を行うことを要旨とする。

【0016】請求項6記載の本発明にあっては、電子データの利用者毎に生成された暗号鍵を用いて暗号化を行う。

【0017】請求項7記載の本発明は、属性情報と本体情報からなる電子データを管理する電子データ管理方法であって、電子データを保存する際に該電子データの利用者を特定するための利用者特定情報と前記電子データを同定するためのデータ同定情報の入力を要求する保存時入力要求過程と、前記電子データを属性情報と本体情報に分割するデータ分割過程と、この分割された属性情報と本体情報を各々異なる記憶領域に格納する格納過程と、前記利用者特定情報、前記電子データに属する前記属性情報および本体情報の前記格納手段におけるそれぞれの格納位置を統合して管理情報として記録管理する記録管理過程と、前記電子データを利用する際に該電子データの利用を要求する利用者を特定するための利用者要求情報と前記電子データを同定するためのデータ同定情報の入力を要求する利用時入力要求過程と、前記利用者要求情報と前記利用者特定情報が一致する場合、前記管理情報を参照して前記格納手段から属性情報と本体情報を読み出し、この読み出した属性情報と本体情報を統合する統合過程とを有し、前記電子データが格納されているときに前記本体情報の所在のみを利用者に開示することを要旨とする。

【0018】請求項7記載の本発明にあっては、電子データを保存する際にパスワード等の利用者特定情報とファイル名等のデータ同定情報の入力を要求し、電子データを属性情報と本体

情報を各々異なる記憶領域に格納し、利用者特定情報、属性情報および本体情報のそれぞれの格納位置を統合して管理情報として記録管理し、また電子データを利用する際にデータ利用者を特定する利用者要求情報とデータ同定情報の入力を要求し、利用者要求情報と利用者特定情報が一致する場合、管理情報を参照して属性情報と本体情報を読み出し、この属性情報と本体情報を統合し、電子データが格納されているときに本体情報の所在のみを利用者に開示する。

【００１９】また、請求項８記載の本発明は、請求項７記載の発明において、前記格納過程が、前記属性情報と本体情報を各々異なる記憶領域に格納するに当り、前記利用者特定情報に基づいた暗号化情報を用いて、前記属性情報と本体情報のいずれか一方または両方を暗号化する暗号化過程を有し、前記統合過程が、前記属性情報と本体情報を統合するに当り、前記利用者要求情報に基づいた復号化情報を用いて、前記暗号化されているいずれか一方または両方の属性情報と本体情報を復号化する復号化過程を有することを要旨とする。

【００２０】請求項８記載の本発明にあっては、属性情報と本体情報を各々異なる記憶領域に格納するに当り、利用者特定情報に基づいた暗号化情報を用いて属性情報と本体情報のいずれか一方または両方を暗号化し、また属性情報と本体情報を統合するに当り、利用者要求情報に基づいた復号化情報を用いて、前記暗号化されているいずれか一方または両方の属性情報と本体情報を復号化する。

【００２１】更に、請求項９記載の本発明は、請求項８記載の発明において、前記暗号化情報および復号化情報が、前記属性情報および本体情報に対して異なる情報であることを要旨とする。

【００２２】請求項９記載の本発明にあっては、暗号化情報および復号化情報は属性情報および本体情報に対して異なる情報である。

【００２３】請求項１０記載の本発明は、属性情報と本体情報からなる電子データを管理する電子データ管理方法であって、電子データを属性情報と本体情報に分割し、この分割された属性情報と本体情報をそれぞれ異なる記憶領域に格納する格納過程を有することを要旨とする。

【００２４】請求項１０記載の本発明にあっては、電子データを属性情報と本体情報に分割し、この分割された属性情報と本体情報をそれぞれ異なる記憶領域に格納するため、電子データを安全に保存することができる。

【００２５】また、請求項１１記載の本発明は、請求項１０記載の発明において、前記格納過程が、前記属性情報と本体情報をそれぞれ異なる記憶領域に格納するに当り、前記属性情報と本体情報のいずれか一方または両方を暗号化する暗号化過程を有することを要旨とする。

【００２６】請求項１１記載の本発明にあっては、属性情報と本体情報をそれぞれ異なる記憶領域に格納するに当り、属性情報と本体情報のいずれか一方または両方を暗号化する。

【００２７】更に、請求項１２記載の本発明は、請求項１１記載の発明において、前記暗号化過程が、前記電子データの利用者毎に生成された暗号鍵を用いて暗号化を行うことを要旨とする。

【００２８】請求項１２記載の本発明にあっては、電子データの利用者毎に生成された暗号鍵を用いて暗号化を行う。

【００２９】請求項１３記載の本発明は、属性情報と本体情報からなる電子データを管理する電子データ管理プログラムを記録した記録媒体であって、電子データを保存する際に該電子データの利用者を特定するための利用者特定情報と前記電子データを同定するためのデータ同定情報の入力を要求する保存時入力要求過程と、前記電子データを属性情報と本体情報に分割するデータ分割過程と、この分割された属性情報と本体情報を各々異なる記憶領域に格納する格納過程と、前記利用者特定情報、前記電子データに属する前記属性情報および本体情報の前記格納手段におけるそれぞれの格納位置を統合して管理情報として記録管理する記録管理過程と、前記電子データを利用する際に該電子データの利用を要求する利用者を特定するための利用者要求情報と前記電子データを同定するためのデータ同定情報の入力を要求する利用時入力要求過程と、前記利用者要求情報と前記利用者特定情報が一致する場合、前記管理情報を参照して前記格納手段から属性情報と本体情報を読み出し、この読み出した属性情報と本体情報を統合する統合過程とを有し、前記電子データが格納されているときに前記本体情報の所在のみを利用者に開示する電子データ管理プログラムを記録媒体に記録することを要旨とする。

【００３０】請求項１３記載の本発明にあっては、電子データを保存する際にパスワード等の利用者特定情報とファイル名等のデータ同定情報の入力を要求し、電子データを属性情報と本体情報に分割し、この属性情報と本体情報を各々異なる記憶領域に格納し、利用者特定情報、属性情報および本体情報のそれぞれの格納位置を統合して管理情報として記録管理し、また電子データを利用する際にデータ利用者を特定する利用者要求情報とデータ同定情報の入力を要求し、利用者要求情報と利用者特定情報が一致する場合、管理情報を参照して属性情報と本体情報を読み出し、この属性情報と本体情報を統合し、電子データが格納されているときに本体情報の所在のみを利用者に開示する電子データ管理プログラムを記録媒体に記録しているため、該記録媒体を用いて、その流通性を高めることができる。

【００３１】また、請求項１４記載の本発明は、請求項１３記載の発明において、前記格納過程が、前記属性情報と本体情報を各々異なる記憶領域に格納するに当り、

前記利用者特定情報に基づいた暗号化情報を用いて、前記属性情報と本体情報のいずれか一方または両方を暗号化する暗号化過程を有し、前記統合過程が、前記属性情報と本体情報を統合するに当り、前記利用者要求情報に基づいた復号化情報を用いて、前記暗号化されているいずれか一方または両方の属性情報と本体情報を復号化する復号化過程を有する電子データ管理プログラムを記録媒体に記録することを要旨とする。

【００３２】請求項１４記載の本発明にあっては、属性情報と本体情報を各々異なる記憶領域に格納するに当り、利用者特定情報に基づいた暗号化情報を用いて属性情報と本体情報のいずれか一方または両方を暗号化し、また属性情報と本体情報を統合するに当り、利用者要求情報に基づいた復号化情報を用いて、前記暗号化されているいずれか一方または両方の属性情報と本体情報を復号化する電子データ管理プログラムを記録媒体に記録しているため、該記録媒体を用いて、その流通性を高めることができる。

【００３３】更に、請求項１５記載の本発明は、請求項１４記載の発明において、前記暗号化情報および復号化情報が、前記属性情報および本体情報に対して異なる情報である電子データ管理プログラムを記録媒体に記録することを要旨とする。

【００３４】請求項１５記載の本発明にあっては、暗号化情報および復号化情報は属性情報および本体情報に対して異なる情報である電子データ管理プログラムを記録媒体に記録しているため、該記録媒体を用いて、その流通性を高めることができる。

【００３５】請求項１６記載の本発明は、属性情報と本体情報からなる電子データを管理する電子データ管理方法であって、電子データを属性情報と本体情報に分割し、この分割された属性情報と本体情報をそれぞれ異なる記憶領域に格納する格納過程を有する電子データ管理プログラムを記録媒体に記録することを要旨とする。

【００３６】請求項１６記載の本発明にあっては、電子データを属性情報と本体情報に分割し、この分割された属性情報と本体情報をそれぞれ異なる記憶領域に格納する電子データ管理プログラムを記録媒体に記録しているため、該記録媒体を用いて、その流通性を高めることができる。

【００３７】また、請求項１７記載の本発明は、請求項１６記載の発明において、前記格納過程が、前記属性情報と本体情報をそれぞれ異なる記憶領域に格納するに当り、前記属性情報と本体情報のいずれか一方または両方を暗号化する暗号化過程を有する電子データ管理プログラムを記録媒体に記録することを要旨とする。

【００３８】請求項１７記載の本発明にあっては、属性情報と本体情報をそれぞれ異なる記憶領域に格納するに当り、属性情報と本体情報のいずれか一方または両方を暗号化する電子データ管理プログラムを記録媒体に記録しているため、該記録媒体を用いて、その流通性を高めることができる。

【００３９】更に、請求項１８記載の本発明は、請求項１７記載の発明において、前記暗号化過程が、前記電子データの利用者毎に生成された暗号鍵を用いて暗号化を行う電子データ管理プログラムを記録媒体に記録することを要旨とする。

【００４０】請求項１８記載の本発明にあっては、電子データの利用者毎に生成された暗号鍵を用いて暗号化を行う電子データ管理プログラムを記録媒体に記録しているため、該記録媒体を用いて、その流通性を高めることができる。

【００４１】

【発明の実施の形態】以下、図面を用いて本発明の実施の形態について説明する。図１は、本発明の一実施形態に係る電子データ管理装置の構成を示すブロック図である。本実施形態は、電子計算機のオペレーションシステム（ＯＳと略称する）にWindows を用いたパーソナルコンピュータ（以下パソコンと略称する）における電子データ管理方法に適用したものである。

【００４２】図１に示す電子データ管理装置は、アプリケーション毎の属性情報と本体情報であるデータ本体からなる電子データであるファイルの保存および閲覧を管理する装置であり、ファイルの入出力を行う入出力部４０１、ファイルである電子データを属性情報とデータ本体に分割するデータ分割部４０２、電子データを暗号化する暗号部４０３、電子データの保存および管理を制御する保存部４０４、電子データの管理情報を記録管理する管理部４０５、電子データから分割された属性情報とデータ本体をそれぞれ異なる格納領域に格納する蓄積部４０７、電子データを蓄積部４０７から取得する取得部４１０、暗号化された電子データを復号する復号部４１１、および復号された属性情報とデータ本体を統合するデータ統合部４１２から構成されている。

【００４３】なお、Windows は、個人で使用するために作られた電子計算機のＯＳであるため、登録された複数のユーザの中から特定のユーザを認証する必要がない。唯一起動時に行っている認証は、Windows 同士のネットワークサービスを利用するための認証であり、パソコンの記憶装置に蓄積された電子データであるファイルを保護する目的のものでない。そのため、Windows を搭載したパソコンでは、悪意のある第三者が閲覧、改変、破壊することは容易である。

【００４４】そこで、本実施形態では、記憶装置内にあるファイルを保護するために、属性情報とデータ本体からなるファイルをそれぞれ属性情報とデータ本体に分離して保存するようにしている。更に詳しくは、図２に示すＧＩＦ画像の電子データ１０１を参照して説明する。ＧＩＦ画像は、一般にヘッダ、論理画面記述子、イメージ記述子から構成される。この場合、属性情報１０２

は、ヘッダと論理画面記述子であり、データ本体１０３はイメージ記述子である。属性情報１０２は、ヘッダとして１行目の「ＧＩＦ８７ａ」がＧＩＦのバージョンを示しており、２行目の「２５６」は幅の画素数を示しており、３行目の「２５６」は縦の画素数を示している。４行目の「０，４，０，１」は、背景色を表示するためのカラーテーブル、画像に使われる色素のパレット全体の大きさ、色の選択順位、カラーテーブルのサイズをそれぞれ示している。５行目の「０」はイメージに含まれない画面上のピクセルに使用される色を示し、６行目の「０」はピクセルの縦横比を示している。

【００４５】データ本体１０３であるイメージ記述子はＲＧＢのデータが交互に並んでいる。このためデータ本体１０３だけでは元のデータである画像を正しく表示することができない。

【００４６】上述したように、電子データ１０１は、属性情報１０２とデータ本体１０３から構成されるが、図１に示す実施形態では、電子データを構成するファイルを属性情報とデータ本体に分割して格納管理するようにしている。

【００４７】すなわち、図１の電子データ管理装置において、ファイルを保存閲覧するには、入出力部４０１を介してファイルの入出力を行い、この入出力部４０１から入力されたファイルはデータ分割部４０２に供給される。データ分割部４０２は、入力されたファイルの属性情報とデータ本体とをそれぞれ図２に示すように分離する。この分離された属性情報とデータ本体は暗号部４０３で暗号化され、保存部４０４に供給される。保存部４０４は、蓄積部４０７に属性情報４０８とデータ本体４０９を保存し、属性情報４０８とデータ本体４０９のそれぞれの保存場所を管理部４０５に登録する。すなわち、管理部４０５は、蓄積部４０７に格納されている属性情報４０８とデータ本体４０９が蓄積されている保存場所の管理を行う。

【００４８】管理部４０５で管理される管理情報４０６は、図３に示すように、各電子データに対して属性情報４０８とデータ本体４０９の保存場所を示すデータで構成されている。例えば、データ番号Ｄ００１の電子データは、属性情報がａａａ００１に、データ本体がｂｂｂ０２１に保存されていることを示している。ただし、保存場所を示すデータは蓄積部４０７内の蓄積場所を示すデータであれば、メモリの番地であってもポインタであってもよく、その実施方法は問わない。

【００４９】次に、取得部４１０は、管理部４０５の電子データ管理情報４０６を基に蓄積部４０７に保存された属性情報４０８とデータ本体４０９を取得する。復号部４１１は、暗号化されたデータを復号し、データ統合部４１２へ渡す。データ統合部は属性情報４０８とデータ本体４０９を統合し、入出力部４０１へ渡す。

【００５０】次に、以上のように構成される電子データ管理装置の作用を図４、図５に示すフローチャートを参照して説明する。

【００５１】まず、図４を参照して、アプリケーション毎の属性情報をデータ本体からなる電子データであるファイルを保存する場合の作用について説明する。入出力部４０１から入力されたファイルは、データ分割部４０２で属性情報とデータ本体に分離され（ステップＳ２０１）、この分離された属性情報とデータ本体は、暗号部４０３においてそれぞれ異なる暗号鍵を用いて暗号化される（ステップＳ２０２）。それから、この暗号化された属性情報とデータ本体は、保存部４０４により蓄積部４０７のそれぞれ別々の格納場所に保存されるとともに、その格納場所を示す電子データ管理情報は管理部４０５に登録される（ステップＳ２０３）。なお、属性情報とデータ本体の暗号化は同じ暗号鍵を用いてもよいし、また属性情報とデータ本体の暗号化の順序は任意である。

【００５２】ファイル暗号化の暗号鍵は、ユーザ毎に生成し、前記暗号鍵は暗号化された状態でＯＳが管理する。ＯＳを起動した時点でユーザ名とパスワードによるユーザ認証を行い、正当なユーザであることが証明されると、暗号化されたファイル暗号化用暗号鍵を復号し、取得する。

【００５３】次に、図５を参照して、ファイルを閲覧する場合の作用について説明する。正当なユーザが特定のアプリケーションを用いてファイルを閲覧する場合には、管理部４０５に登録されている管理情報に基づいて蓄積部４０７から暗号化された属性情報とデータ本体を取得部４１０により取得する（ステップＳ３０１）。それから、この暗号化された属性情報とデータ本体を復号部４１１でそれぞれ復号する（ステップＳ３０２）。次に、この復号された属性情報とデータ本体をデータ統合部４１２で統合し（ステップＳ３０３）、入出力部４０１から出力する。なお、復号鍵の管理は暗号鍵と同じように暗号化された状態でＯＳが管理する。

【００５４】次に、本発明の他の実施形態として、電子計算機のＯＳにＵＮＩＸを用いたワークステーションにおける電子データ管理方法に適用した場合について説明する。

【００５５】ＵＮＩＸは複数のユーザが使うことが前提に作られたＯＳであるため、ユーザのＩＤやパスワードを管理者で一括管理を行っている。そのため、悪意のある第三者に一括管理されたＩＤとパスワードを奪取されると、すべてのユーザのデータが閲覧、改変、または破壊することが容易に可能となる。

【００５６】そこで、図１の実施形態と同じ方法にてファイルを管理する。もちろん、ファイル暗号化の暗号鍵は、ユーザ毎に生成し、前記暗号鍵は暗号化された状態でＯＳが管理する。ＵＮＩＸにログインした時点でユーザ名とパスワードによるユーザ認証を行い、正当なユー

ザであることが証明されると、暗号化されたファイル暗号化用暗号鍵を復号し、取得する。ただし暗号化の方法は問わない。

【００５７】

【発明の効果】以上説明したように、本発明によれば、電子データを属性情報と本体情報に分割し、この分割された属性情報と本体情報をそれぞれ異なる記憶領域に格納し、また異なる記憶領域に格納するに当り属性情報と本体情報のいずれか一方または両方を利用者毎に生成された暗号鍵で暗号化を行うので、電子データの安全性を向上し、第三者による電子データの閲覧、盗用等を適確に防止することができるとともに、ネットワーク上で複数の電子計算機を用いて安全性の高い電子データ共有や配送が可能となる。特に、電子データを分離する方法をネットワーク上に用いることにより安全性の高いデータ通信が可能となる。

【図面の簡単な説明】

【図１】本発明の一実施形態に係る電子データ管理装置の構成を示すブロック図である。

【図２】図１の実施形態で管理する電子データおよびその分割された属性情報とデータ本体を示す図である。

【図３】図１の実施形態の管理部で管理される電子データ管理情報の構成を示す図である。

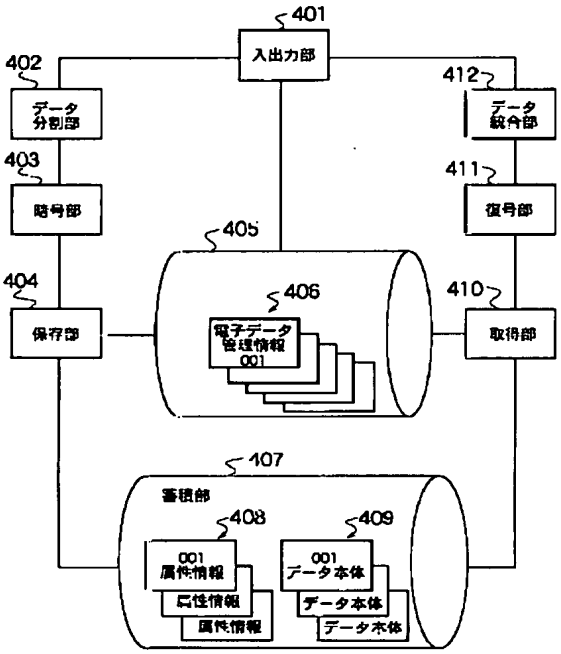
【図４】図１の実施形態における電子データの保存処理を示すフローチャートである。

【図５】図１の実施形態における電子データの取得処理を示すフローチャートである。

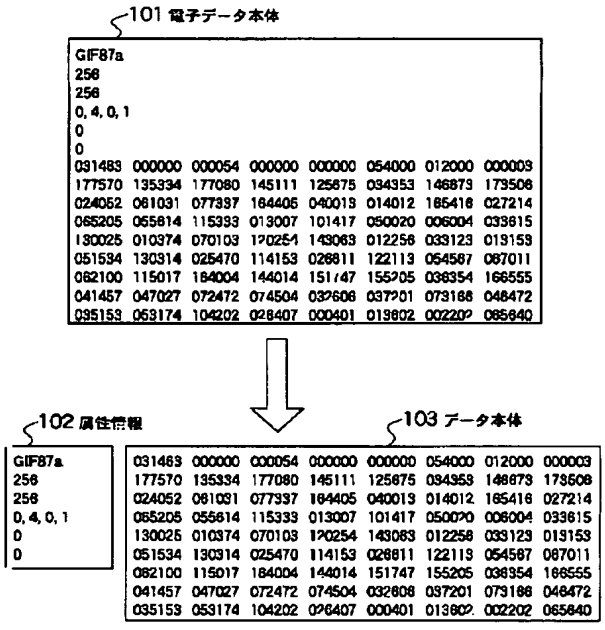
【符号の説明】

４０１　入出力部
４０２　データ分割部
４０３　暗号部
４０４　保存部
４０５　管理部
４０７　蓄積部
４１０　取得部
４１１　復号部
４１２　データ統合部

【図１】



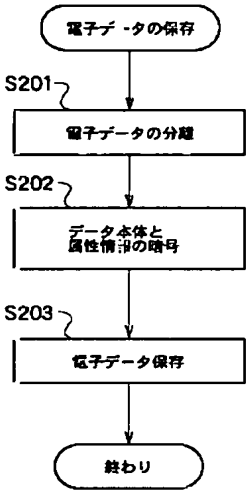
【図２】



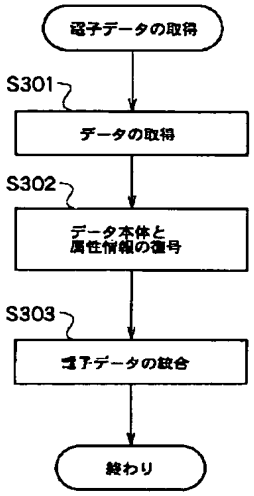
【図３】

電子データ管理		
データ番号	属性情報（Z）	データ本体（H）
001	aaa001	bbb021
002	ccc001	ddd021
003	ddd001	ccc021
004	eee001	eee021
005	bbb001	aaa021

【図4】



【図5】



フロントページの続き

(72)発明者　渡部　保日児
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内
(72)発明者　曽根原　登
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内

Ｆターム(参考)　5B017 AA01 BA05 BA07 BA10 CA16
5J104 AA07 AA12 KA01 KA04 NA38 PA07 PA14
9A001 EE03 HH23 HH31 JJ01 LL03 LL09